UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/496,065	02/01/2000	N. Asokan	SZ998-041	5668

7590 02/07/2006

Anne Vachon Dougherty Esq
IBM Corp
3173 Cedar Rd
Yorktown Heights, NY 10598

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 02/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/496,065	**Applicant(s)** ASOKAN ET AL.
	Examiner Michael J. Simitoski	**Art Unit** 2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 November 2005*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *9-14,16-26 and 30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *9-14,16-26 and 30* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 February 2004* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. The response of 11/28/2005 was received and considered.

2. Claims 9-14, 16-26 & 30 are pending.

Response to Arguments

3. Applicant's response (p. 12) argues that the prior art fails to teach a server communicating information directly to the user device along a connection between the server and the user device. However, this claim language is indefinite and is not enabled by the specification. Specifically, "directly" is not defined.

4. Applicant's response (p. 12) argues that the prior art fails to teach terminal authentication information being communicated to the user, whereupon the user or the user device provides information to the terminal for the terminal to dynamically create a user-specific authenticity output message for display to the user. However, this generic claim language is indefinite and is not enabled by the specification. Specifically, "dynamically" is not defined. The specification on p. 20 (last ¶) states that "Another variation is where the user 1 challenges T to show a different component of the authentication vector each time." *Therefore, for the purposes of this Office Action, "dynamically create a user-specific authenticity output message" is understood to mean that the authenticity output message is not always the same.*

5. Applicant's response (p. 14) argues that in Merritt does not generate a message that is send to the user along a connection which is separate from the connection between the host and the terminal. Applicant's response further argues that the user does not have a separate connection with the host and does not receive terminal authentication information from the host. However, as stated previously, the specification provides no direction as to how to explicitly

define a connection and as to what makes the connections separate. On p. 10, #4, ¶1 of the instant specification, S-D is tunneled through S-T. This means that the S-D connection travels along the same path as the S-T; the difference is that S-D travels further (to a further destination, rather than stopping at T) (see also #5, line 2). Because Merritt discloses that the mutual authentication is performed between the terminal and host (first connection) and the message is communicated back from the user (second connection), applicant's arguments are not persuasive.

6. Applicant's response (p. 14) argues that the Merritt server does not authenticate the terminal. However, the terminal and the server participate in mutual authentication, indicating that each device is authenticated to the other (Fig. 3).

7. Applicant's response (p. 14) argues that the server does not generate any authenticity output message regarding the authenticity of the terminal. However, the claims do not recite a limitation requiring the output message indicating the authenticity of the terminal. Further, because the message is output only after the terminal and the host both engage in mutual authentication, the message indicates that the terminal is authentic (Fig. 3).

8. Applicant's response (p. 15) argues that Merritt does not teach a first and second trusted connection. However, this has been addressed above.

9. Applicant's response (p. 15) argues that the limitation "separate" is disclosed in the specification. However, Applicant's response has not drawn attention to any definition of separate. For instance, if separate were to indicate different physical means of communication, the specification does not support this. It is maintained that the language regarding "separate" connections is not described in the specification and that the specification does not enable one of ordinary skill in the art to make and use an invention with separate connections.

10. Applicant's response (p. 16) argues that Merritt's server does not teach that the components comprise an authentication component for verifying the authenticity of the terminal. However, applicant's attention is drawn to Fig. 4 where Merritt discloses the calculations at both the ATM and host to mutually authenticate. In step 335, the host determines that the ATM is authenticated.

11. Applicant's response (p. 17) argues that Merritt does not teach a host server that has a message generation component or that the server generates an authenticity output message. However, as seen in Fig. 5, the host decrypts the account info and retrieves the PSP/authenticity output message. Applicant's response (p. 17) also argues that "it is clear that the Merritt element 3 database is not a message generation component but is simply a storage location." However, applicant's specification shows a similar structure to Merritt where the authenticity output message is read from a stored message (p. 13, ¶1). Further, by decrypting the account info and retrieving the PSP, Merritt is generating an authenticity output message.

12. Applicant's response (pp. 18-19) argues that the PSP is not a terminal authenticity message. However, as stated above, because the message is output only after the terminal and the host both engage in mutual authentication, the message indicates that the terminal is authentic (Fig. 3).

13. Applicant's response (p. 19) argues that sending terminal authentication information directly from a server to a user device along a connection which is separate from the connection between the terminal and the server, thereby eliminating the possibility of a terminal interfering with or falsely generating a terminal authentication message, is not taught or suggested by the Manduley device display. It is noted that, "thereby eliminating ..." (while only reciting intended

use) is not recited in the claims; if applicant intends to rely on this language, the language must be reflected in the claims. Further, Manduley teaches that exchanging messages between a user and a card is important because it ensures that the correct user is using the card (col. 1, lines 41-56 & col. 2, lines 7-23). Using a smartcard is beneficial over Merritt's standard credit/debit card, which does not authenticate the user. The smartcard contains an LCD display to which the server sends an authenticity message to the user (col. 3, lines 11-16, lines 47-58). In this case, the smartcard is acting as a second interface to the server (rather than just the terminal), where the server sends an authenticity message accepting both the user and the card to the card (col. 4, lines 22-41). Therefore, it would be obvious to modify Merritt's invention to send the authenticity message of Merritt along with the authenticity message of the smart card to the smart card in one message. One of ordinary skill in the art would have been motivated to perform such a modification to gain the additional benefit of authenticating the card to the user and the card and user to the server.

14. Applicant's response further argues that the references cited fail to teach a message communicated directly to the user device along a separate connection, without also communicating the message along the connection between the terminal and the server. However, as previously stated, the specification gives no direction on what a "direct" connection is (physical link, courier, etc.). Further, the specification does not define what makes one connection "separate" from another (different time, different source/destination combinations, etc.). Further, the specification provides no support for a device that sends a message along one connection between the server and user device without also sending it along the connection between the terminal and the server. As discussed above, the specification (p. 10 for example)

discloses sending the message from the server to the terminal and from the terminal to the device.

15. Applicant's response (p. 21) argues that none of the cited references teach two different connections. As stated previously, applicant has not defined different or separate connections. There are multiple interpretations, for instance a connection can be defined as a source and a destination – therefore a single transaction in one direction is a different connection than one in the other direction. A different connection could be defined as being outside a certain timeframe from a first connection. A different connection could be defined as a different physical transmission medium from a first connection. A different connection could be defined as a transmission between source and an intended receiver. The multiple interpretations are neither established in the art, nor explicitly defined in the instant application. Applicant's further argues that none of the references teach providing a message via an established second connection between the user device and the terminal without also communicating that message to the terminal along the first connection. However, Applicant's specification clearly shows S-D being tunneled through S-T, i.e. the message traveling to the terminal and then to the device (p. 10). As such, Merritt teaches that the PSP is communicated to the user via the terminal and as modified, to the device, via the terminal (Fig. 3).

16. Applicant's response (p. 21) argues that Schneier does not teach communication of terminal authentication along a connection between a server and a user device and not along a different connection between the terminal and the server. However, Schneier is not relied upon for teaching these limitations.

17. Applicant's response (p. 22) argues that the combination of Merritt, Manduley and Lessin would again effectively teach away from the claimed invention since the user would be forced to enter his PIN at a terminal before establishing that the terminal was trusted. However, Lessin suggests entering the PIN into the device, which is trusted and therefore would not teach away. Furthermore, Lessin does not teach away from the combination of Merritt, Manduley and Hoss for the same reason.

Claim Objections

18. Claims 9-26 are objected to because of the following informalities:

Regarding claim 9, line 3, “via a user input device, comprising” should be replaced with “”via a user input device, the server comprising”.

Regarding claim 12, line 5, “said user device, comprising” should be replaced with “said user device, the method comprising”

Appropriate correction is required.

Specification

19. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: The terms “directly” and “dynamically” are not disclosed.

Claim Rejections - 35 USC § 112

20. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

21. Claims 9-26 & 30 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

a. The specification does not disclose the first trusted connection being separate from the second trusted connection and that the message is not delivered over the first trusted connection between the terminal and the server.

b. The specification does not disclose "dynamically" generating an authenticity output message.

c. The specification does not disclose delivery of an authenticity message "directly" to a user device.

22. Claims 9-26 & 30 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

d. The specification does not enable one of ordinary skill to "separate" the two connections and does not disclose how data is sent over one trusted connection without sending the data over the other.

e. The specification does not define "dynamically" creating an authenticity message in such a manner that would enable one having ordinary skill in the art to make the invention.

f. The specification does not define "directly" in such a manner that would enable one having ordinary skill in the art to make the invention.

23. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

24. Claims 18 & 22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The claims depend on claim 15, which is cancelled. *For the purposes of this Office Action, claims 18 & 22 are understood to depend from claim 13.*

25. For the purpose of advancing prosecution of the instant application, the claims are rejected as best understood in light of the preceding 112 rejections.

Claim Rejections - 35 USC § 103

26. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

27. Claims 9-14, 16-18, 21-22, 25-26 & 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 5,475,756 to **Merritt** in view of U.S. Patent 5,737,423 to **Manduley**, U.S. Patent 5,412,192 to **Hoss** and U.S. Patent 5,793,952 to **Limsico**.

Regarding claims 9, 11-12, 14, 17, 21, 30, Merritt discloses a server/host (Fig. 1, #2), a communications component/communication line (col. 2, lines 48-64) for establishing and conducting communications along a first trusted connection with the terminal (Fig. 1, #9) and along a second trusted connection with said user input device (data transfers from the user's card to the host through the ATM) (Fig. 1, #9, col. 4, lines 46-51 & col. 6, lines 21-22) wherein the first trusted connection is separate from the second trusted connection (each have unique source/destination), receiver means for receiving at least one authentication request from said terminal (Fig. 3, #310 & #360), at least one authentication component for verifying the authenticity of the terminal (Fig. 1, #4, #8, Fig. 3, #315 & col. 4, line 58 – col. 5, line 17) and a message generation component for generating at least one authenticity output message/PSP (col. 4, lines 11-20) for delivery (from host to ATM screen) (Fig. 1, #3) and a storage location (Fig. 1, element 3) for storing a user-specific authenticity output message/PSP (col. 4, lines 11-20). Merritt lacks sending the authenticity output message to the device (user's card) over the second connection. However, Manduley teaches that smart cards are useful in secure transactions, particularly as an electronic purse (col. 1, lines 11-29) and that exchanging messages between a user and a smart card is useful to make sure the correct user is using the smart card (col. 2, lines 7-23 & col. 1, lines 41-56). More specifically, Manduley teaches that the smartcard contains an LCD display that will, at the request of the server/issuing authority, display a message to the user (col. 3, lines 11-16, lines 47-58). This message can be a message requesting the user to enter a response (col. 3, lines 47-58) to authenticate the user's presence (col. 4, lines 7-15). The response is encrypted, thereby authenticating the card (col. 2, lines 7-15 & col. 4, lines 7-13). In this situation, the smart card is acting as a second interface to the server (rather than just the terminal). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Merritt to send the authenticity output message to a smart card (second trusted connection). One of ordinary skill in the art would have been motivated to perform such a modification because smart cards are used in secure transactions to ensure the legitimate user of the card will be reading the messages and allow the user to respond, as taught by Manduley (col. 2, lines 7-23 & col. 1, lines 41-56). Merritt, as modified, lacks explicitly not sending the message along the first trusted connection between the terminal and the server. However, Hoss teaches that to allow a remote source to control a smart card at any time (col. 1, lines 29-32, col. 2, lines 1-7 & lines 1-59), the card contains an RF receiver that can display messages to the user (Fig. 1 & col. 3, lines 11-17). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Merritt to send the authenticity message/PSP directly to the smart card over an RF link. One of ordinary skill in the art would have been motivated to perform such a modification to maintain access to the card anywhere, as taught by Hoss (col. 1, lines 29-32 & lines 54-66). As modified, Merritt lacks the user-specific authenticity output message/PSP being dynamically generated. However, Limsico teaches that user passwords should be changed on a regular basis to increase the level of security of a user's account (col. 1, lines 54-58). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Merritt to change the user's password/PSP on a regular basis. One of ordinary skill in the art would have been motivated to perform such a modification to increase the level of security of a user's account, as taught by Limsico (col. 1, lines 54-58).

Regarding claim 10, Merritt discloses the host and the terminal negotiating a session key (col. 6, lines 54-62).

Regarding claim 13, Merritt discloses communicating a message to a user (Fig. 5, element 515).

Regarding claim 15, as best understood, Merritt discloses a terminal displaying a message (col. 3, lines 40-45).

Regarding claim 16, Merritt discloses accessing a database/lookup table that stores user-specific messages/PSPs (col. 7, lines 1-10).

Regarding claim 18, Merritt discloses authentication information contained on the card (col. 3, lines 64-67 and col. 4, lines 1-11) to be read by the terminal/ATM (Fig. 3). Merritt discloses a terminal displaying an authenticity output message/PSP in response to authentication (Fig. 5 and col. 3, lines 20-48).

Regarding claim 22, Merritt discloses a message/PSP taking many forms, such as a still image, a sequence of images, a video or an audio clip (col. 4, lines 16-23).

Regarding claim 25, Merritt discloses a smart card system, as described above, but lacks authenticating the card to the server. However, Manduley teaches that a smart card should be periodically authenticated by the issuing authority/server (col. 3, line 64 – col. 4, line 21) to allow the issuing authority/server to maintain control over issued cards (col. 1, lines 30-54). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to authenticate the user device to the server. One of ordinary skill in the art would have been motivated to perform such a modification to maintain control over issued cards, as taught by Manduley (col. 1, lines 30-54).

Regarding claim 26, Merritt discloses authenticating a user (Fig. 3, element 390).

28. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Merritt** in view of **Manduley, Hoss & Limsico,** as applied to claim 12 above, in further view of U.S. Patent 4,799,061 to Abraham et al. (**Abraham**). Merritt, as modified, lacks the device authenticating itself to the terminal. However, Abraham teaches that components in a communication system should be authenticated prior to communicating any useful information (col. 1, lines 62-66 & col. 2, lines 4-16), specifically between a smart card and a terminal (Fig. 1) to protect against usage of an unauthorized terminal (col. 1, line 66 – col. 2, line 3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Merritt to require the smart card authenticate itself to the terminal. One of ordinary skill in the art would have been motivated to perform such a modification to protect against usage of an unauthorized terminal, as taught by Abraham (col. 1, line 62 – col. 2, line 16).

29. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Merritt** in view of **Manduley, Hoss & Limsico,** as applied to claim 12 above, in further view of U.S. Patent 4,868,376 to Lessin et al. (**Lessin**). Merritt discloses a smart card system, as described above, but lacks the card requesting the user authenticate himself. Lessin teaches that by requiring the user enter a PIN, a card can prevent unauthorized access to data (col. 4, lines 7-11 and col. 8, lines 27-41). Therefore, it would have been obvious to one having ordinary skill in the art at the

time the invention was made to modify Merritt's smart card system to request the user authenticate himself to prevent unauthorized access. One of ordinary skill in the art would have been motivated to perform such a modification to prevent unauthorized access to data on the card, as taught by Lessin.

30. Claims 23 & 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Merritt** in view of **Manduley, Hoss & Limsico**, as applied to claim 21 above, in further view of **Schneier**. Merritt, as modified above, lacks partially outputting a message. However, Schneier teaches that SKEY is a known authentication protocol (as the PSP is used to authenticate the server/host). In SKEY, each entity has a list of numbers (message). One of the numbers is outputted to be recognized by the other entity (partial message) (page 53). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the SKEY protocol for authentication using a message/PSP. One of ordinary skill in the art would have been motivated to perform such a modification because an eavesdropper gains no information about the message in that each output of the message is used only once (page 53).

Conclusion

31. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

32. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(571) 273-8300
(for formal communications intended for entry)
Or:
(571) 273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
February 1, 2006

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100